

Microsoft PPTP Server and Client remote vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-09/0309.html>

From: sh@phion.com

Date: 09/26/02

To: bugtraq@securityfocus.com

From: sh@phion.com

Date: Thu, 26 Sep 2002 12:43:46 +0300

phion Security Advisory 26/09/2002

Microsoft PPTP Server and Client remote vulnerability

Summary

The Microsoft PPTP Service shipping with Windows 2000 and XP contains a remotely exploitable pre-authentication bufferoverflow.

Affected Systems

Microsoft Windows 2000 and XP running either a PPTP Server or Client.

Impact

With a specially crafted PPTP packet it is possible to overwrite kernel memory.

A DoS resulting in a lockup of the machine has been verified on Windows 2000 SP3 and Windows XP.

A remote compromise should be possible deploying proper shellcode, as we were able to fill EDI and EDX with our data.

Clients are vulnerable too, because the Service always listens on port 1723 on any interface of the machine, this might be of special concern to DSL users which use PPTP to connect to their modem.

Solution

SecurityFocus Bugtraq: Microsoft PPTP Server and Client remote vulnerability

As a temporary solution for the Client issue, one might firewall the PPTP port in the Internet Connection Firewall for Windows XP.

We dont know of any solution for Windows 2000 and Windows XP PPTP servers.

The vendor has been informed.

Acknowledgements

The bug has been discovered by Stephan Hoffmann and Thomas Unterleitner on behalf of phion Information Technologies.

Contact Information

phion Information Technologies can be reached via:
office@phion.com / <http://www.phion.com>

Stephan Hoffmann can be reached via:
sh@phion.com

Thomas Unterleitner can be reached via:
t.unterleitner@phion.com

References

[1] phion Information Technologies
<http://www.phion.com/>

Exploit

phion Information Technologies will not provide an exploit for this issue.

Disclaimer

This advisory does not claim to be complete or to be usable for any purpose.

This advisory is free for open distribution in unmodified form.

Articles or Publications that are based on information from this advisory have to include link [1].

-
- **Previous message:** grazer@digit-labs.org: "Borland Interbase local root exploit"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)